

Application No.: 10/656,570

Docket No.: 17245/007004

**REMARKS**

Please reconsider the application in view of the above amendments and the following remarks. Applicants thank the Examiner for carefully considering this application. Please note that any references to the text of the instant specification or cited prior art that is a published application are to the published version.

**Disposition of Claims**

Claims 1-26 were pending in the present patent application. By way of this reply, claim 3 has been cancelled without prejudice or disclaimer. Accordingly, claims 1-2 and 4-26 are now pending in the present application. Claims 1, 6, 7, and 26 are independent. The remaining claims depend, either directly or indirectly, from claims 1 and 7.

**Claim Amendments**

Independent claims 1, 6, 7, and 26 have been amended for clarification. Specifically, claims 1, 6, 7, and 26 are amended to make clear that the present invention is directed to a personal computer system as distinguished from a host/server computer system and that the personal computer is secured from malicious code contained in a file downloaded onto the personal computer from an external data source. Further, the dependent claims have been amended to correct antecedent basis issues based on the amendments made to the independent claims and correct other inconsistencies. These amendments have been made for clarification purposes only and no new matter has been introduced by way of these amendments as support for these amendments may be found, for example, in paragraphs [31]-[38] and [40] of the published specification.

**Rejections under 35 U.S.C. § 102**

Claims 1-6 and 26 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Publication No. 2002/0069369 (hereinafter "Tremain"). By way of this reply, claim 3 has been cancelled and thus the rejection is moot as to that claim. As for the remaining claims, for the reasons set forth below, this rejection is respectfully traversed.

Application No.: 10/656,570

Docket No.: 17245/007004

For anticipation under 35 U.S.C. § 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. The Applicants respectfully asserts that that the Office has misconstrued the present invention and/or the teaching of Tremain. Specifically, Applicants assert that Tremain: (1) does not disclose all of the elements (or their equivalents) of instant claim 1 functioning in the same way as the claimed invention; (2) does not disclose each and every element of the claimed invention *arranged as in the* instant claim. Additionally, Applicants assert that there are differences between the claimed invention and Tremain, as viewed by one of ordinary skill in the art at the time of the invention by Applicants.

Specifically, Applicants submit that the apparatus/method of Tremain has no utility without a network connection to a "real network" via which it can provide its "computer services" to a "customer." This is because the Tremain system is a server. *See* Figs. 1, 4-6. Clearly, the computer apparatus of Tremain is a host or server system "providing. . . computer services for a plurality of customers." *See* paragraph [0043] and Abstract of Tremain. Tremain itself asserts this fact in the prosecution of its patent application in its Reply paper dated April 11, 2005 (*see* Exhibit A), where Tremain states on page 13 (and other places) that the problem it addresses and its technical utility is: "to host or provide computer services. . . for plural customers." One of ordinary skill in the art knows the difference between a host/server computer system and a personal computer system. Additionally, the ordinary skilled artisan knows that a host/server computer system requires a network connection in order to be useful to its customers. Without a network connection, Tremain will not function for its intended purpose, and is not a proper reference under 35 U.S.C. §102.

In further contrast, as recited in the amended claims of the present intrusion secure computer system, the invention is directed to personal-type (*i.e.*, standalone) computer system, not a host/server system as taught in Tremain. *See*, for example, paragraphs [0026] and [0027] of published version of the instant specification. The techniques recited in the claims of the present invention do not attempt to protect the network, but rather protect the node (*i.e.*, personal computer system) on the network. Any security provided by Tremain's invention is between the server and the external data sources (*e.g.*, "customers") that solicit information from that server. As noted above the ordinary skilled artisan knows the difference between a host/server computer system and a stand-alone/personal computer system, and that they are neither similar nor

Application No.: 10/656,570

Docket No.: 17245/007004

equivalent in the field. Additionally, the present invention does not require a network connection to accomplish its utility. See Table IA on pages 3-4 of Applicants' Reply paper filed April 17 2005 (Exhibit B). Table IA of Exhibit B shows that the invention of original claim 1 has no such requirement, and its protection features are enabled and function without a server and/or a network (communications channel), because the present invention does not depend on the hostile download coming via a communications channel in order to provide an intrusion secure stand-alone/personal computer system. Omission of an element with retention of the element's function is indicia of unobviousness. *In re Edge*, 359 F.2d 896, 149 USPQ 556 (CCPA 1966).

Accordingly, Tremain does not teach or suggest each and every limitation of amended Claim 1. Claims 6 and 26 contain at least the same limitations as claim 1 and, therefore, should be allowable for at least the same reasons.

In view of the above, independent claims 1, 6, and 26 are patentable over Tremain. The remaining claims depend, either directly or indirectly, from claim 1 and are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

#### Rejections under 35 U.S.C. § 103

Claims 7-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Tremain in view of U.S. Patent No. 6,526,488 issued to White et al. (hereinafter "White"). To the extent this rejection applies to the amended claims, this rejection is respectfully traversed.

To establish a *prima facie* case of obviousness "...the prior art reference (or references when combined) must teach or suggest all the claim limitations." (See MPEP §2143.03). Further, "all words in a claim must be considered in judging the patentability of that claim against the prior art." (See MPEP §2143.03). The Applicant respectfully asserts that the references, when combined, fail to teach or suggest all the claim limitations of amended independent claim 7.

Initially, claim 7 includes substantially the same limitations as claims 1, 6, and/or 26. Accordingly, for the same reasons cited above, Tremain fails to teach or suggest claim 7. Further, White fails to teach what Tremain lacks as is evidenced by the fact that the Examiner

Application No.: 10/656,570

Docket No.: 17245/007004

only cites White to teach "controlling access to corrupt information on a computer system caused by a PC virus." See Office Action dated July 28, 2005 at page 4.

Further, Applicants assert there is no motivation to combine Tremain and White. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must *both* be found in the prior art, *not* in Applicant's disclosure, [*In re Vaack*, 947 F.2d 488 (Fed. Cir. 1991) (emphasis added)] and neither Tremain nor White contain such a teaching or suggestion. Further, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990). In other words, there must be some objective reason to combine the teachings of the reasons. *Ex parte Levengood*, 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993).

As Tremain is concerned with *providing computer services to a plurality of customers over a shared network* (server/host environment) without teaching a protection scheme for data on the host/node (*i.e.*, single computer system) (*see*, Abstract of Tremain) and White is concerned with *controlling access to and corruption of data in a single computer system* (*see*, Abstract of White), a complete study of Tremain and White confirms that, regardless of whether the teachings of Tremain and White *can* be combined, there is no suggestion or motivation set forth in either Tremain and White to combine the teachings of these references. In fact, Tremain is completely silent regarding a virtualization technique to protect data resident on the single computer system; the only virtualization technique taught in Tremain is located on the server side. As shown in paragraph [0202], Tremain teaches a technique that takes place only on a server while the nodes run without virtualization. Absent such a suggestion or motivation, the teachings of Tremain and White cannot be conveniently combined to render the claimed invention obvious.

In view of the above, neither Tremain nor White, individually or in combination, teach or suggest each and every limitation of independent claim 7. Thus independent claim 7 is patentable over Tremain in view of White. The remaining claims depend, directly or indirectly, from claim 7 and are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

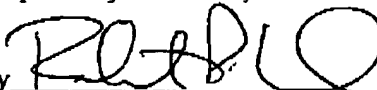
Application No.: 10/656,570

Docket No.: 17245/007004

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. If a fee is due, please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 17245/007004).

Dated: December 28, 2005

Respectfully submitted,

By 

Robert P. Lord  
Registration No.: 46,479  
OSHA • LIANG LLP  
1221 McKinney St., Suite 2800  
Houston, Texas 77010  
(713) 228-8600  
(713) 228-8778 (Fax)  
*Attorney for Applicants*

Attachments (Exhibits A and B)

# EXHIBIT A

**RECEIVED  
CENTRAL FAX CENTER**

DEC 28 2005

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Appl. No. : 09/898,286

Confirmation No. 2215

Applicant : Geoffrey Donald Tremain

Filed : July 3, 2001

TC/A.U. : 2131

Examiner : Eleni A. Shiferaw

Docket No. : 1821-01100

Customer No.: 23505

Title: Method and Apparatus for Providing Computer Service

**AMENDMENT AND RESPONSE TO OFFICE ACTION  
DATED DECEMBER 9, 2004**

Attorney Dkt. No.: 1821-01100

Date: April 11, 2005

Mail Stop Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

In response to the Office Action dated December 9, 2004, please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 12 of this paper.

147983.01/1821.01100

App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

### **Amendments to the Claims**

This listing of claims will replace all prior versions, and listings, of claims in the application:

#### **Listing of Claims:**

1. (Currently amended) Apparatus providing one or more computer services for a plurality of customers, the apparatus comprising a real computer on which is set up at the request of each of said customers at least one virtual machine for each of said customers, said at least one virtual machine for each of said customers having a specification specified by and configurable by the respective customer and having an operating system running thereon.
2. (Original) Apparatus according to claim 1, wherein plural virtual machines are set up within the real computer for at least one of said customers.
3. (Original) Apparatus according to claim 1, wherein the or each virtual machine for at least one of said customers is connected to a virtual network set up for said at least one customer within the real computer.
4. (Original) Apparatus according to claim 3, comprising a virtual intrusion detection device for detecting an attack on the virtual network.
5. (Original) Apparatus according to claim 1, wherein at least one virtual machine is connected to a virtual firewall that is connectable to an external network to which customers and/or other users can connect such that access to said at least one virtual machine by a customer or other user via a said external network can only take place through a virtual firewall.
6. (Original) Apparatus according to claim 1, wherein the or each virtual machine for a particular customer is connected to a virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall being connectable to an external network to which each of said customers and/or other users can connect such that access to a virtual machine by a



App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines.

7. (Original) Apparatus according to claim 6, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall having a second port connected to a virtual network that is set up within the real computer and that is connectable to an external network.

8. (Original) Apparatus according to claim 7, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network.

9. (Original) Apparatus according to claim 5, wherein the or at least one of the virtual firewalls is implemented by a virtual machine on the real computer, said virtual firewall virtual machine running firewall software.

10. (Original) Apparatus according to claim 1, comprising a plurality of real data storage devices and at least one virtual storage subsystem that is configured to allow said real data storage devices to emulate one or more virtual storage devices.

11. (Original) Apparatus according to claim 10, wherein the at least one virtual storage subsystem is configured to emulate at least one respective virtual storage device for each customer.

12. (Original) Apparatus according to claim 10, comprising a detection device for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem.

13. (Original) Apparatus according to claim 1, wherein the apparatus is configurable to provide at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management

App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services.

14. (Original) Apparatus according to claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines.

15. (Original) Apparatus according claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer.

16. (Original) Apparatus according claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network.

17. (Original) Apparatus according to claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer.

18. (Original) Apparatus according claim 1, wherein the real computer comprises plural physical computers.

19. (Original) In combination, a first apparatus according to claim 1 and a second apparatus that is substantially identical to said first apparatus, the first and second apparatus being connected by a communications channel so that the second apparatus can provide for redundancy of the first apparatus thereby to provide for disaster recovery if the first apparatus fails.

20. (Currently amended) A method of providing one or more computer services for a plurality of customers, the method comprising the steps of:

App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

a service provider setting up on a real computer at the request of each of said customers at least one virtual machine for each of said customers, said at least one virtual machine for each of said customers having a specification specified by and configurable by the respective customer and having an operating system running thereon.

21. (Original) A method according to claim 20, comprising the step of setting up plural virtual machines within the real computer for at least one of said customers.

22. (Original) A method according to claim 20, comprising the steps of setting up a virtual network for at least one of said customers within the real computer, and connecting the or each virtual machine for said at least one customer to said virtual network.

23. (Original) A method according to claim 22, comprising the step of using a virtual intrusion detection device for detecting an attack on the virtual network.

24. (Original) A method according to claim 20, comprising the steps of connecting at least one virtual machine to a virtual firewall, and connecting the or each virtual firewall to an external network to which customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall.

25. (Original) A method according to claim 20, comprising the step of connecting the or each virtual machine for a particular customer to a virtual firewall that is dedicated to that customer's virtual machine or machines, and connecting each virtual firewall to an external network to which each of said customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines.

26. (Original) A method according to claim 25, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual

App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

firewall having a second port connected to a virtual network that is set up within the real computer and that is connected to an external network.

27. (Original) A method according to claim 26, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network.

28. (Original) A method according to claim 20, comprising the step of configuring at least one virtual storage subsystem to allow multiple real data storage devices to emulate one or more virtual storage devices.

29. (Original) A method according to claim 28, comprising the step of configuring the at least one virtual storage subsystem to emulate at least one respective virtual storage device for each customer.

30. (Original) A method according to claim 28, comprising the step of using a detection device for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem.

31. (Original) A method according to claim 20, wherein the services provided include at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services.

32. (Original) A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines.

App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

33. (Original) A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer.
34. (Original) A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network.
35. (Original) A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer.
36. (Original) A method according to claim 20, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer.
37. (Currently amended) A method of operating a real computer on behalf of plural customers, the method comprising the step of:  
operating plural virtual machines on the real computer, each of said plural virtual machines having a specification specified by and configurable by a respective one of the customers in accordance with a computer service to be provided by the virtual machine on behalf of that customer, each of said virtual machines having an operating system running thereon.
38. (Original) A method according to claim 37, comprising the step of operating plural virtual machines within the real computer for at least one of said customers.
39. (Original) A method according to claim 37, comprising the step of operating a virtual network for at least one of said customers within the real computer, the or each virtual machine for said at least one customer being connected to said virtual network.
40. (Original) A method according to claim 39, comprising the step of using a virtual intrusion detection device for detecting an attack on the virtual network.

App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

41. (Original) A method according to claim 37, wherein at least one virtual machine is connected to a virtual firewall, the or each virtual firewall being connected to an external network to which customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall.

42. (Original) A method according to claim 37, wherein the or each virtual machine for a particular customer is connected to a virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall being connected to an external network to which each of said customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines.

43. (Original) A method according to claim 42, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall having a second port connected to a virtual network that is set up within the real computer and that is connected to an external network.

44. (Original) A method according to claim 43, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network.

45. (Original) A method according to claim 37, wherein at least one virtual storage subsystem is provided and configured to allow multiple real data storage devices to emulate one or more virtual storage devices.

46. (Original) A method according to claim 45, wherein the at least one virtual storage subsystem is configured to emulate at least one respective virtual storage device for each customer.

App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

47. (Original) A method according to claim 45, wherein a detection device is used for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem.

48. (Original) A method according to claim 37, wherein the services provided include at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services.

49. (Original) A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines.

50. (Original) A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer.

51. (Original) A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network.

52. (Original) A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer.

53. (Currently amended) A method according to claim ~~37~~ 53, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer.

App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

54. (Currently amended) A method of providing for a plurality of customers one or more computer services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services; the method comprising the steps of:

setting up on a real computer at the request of each of said customers at least one virtual machine for each of said customers, said at least one virtual machine for each of said customers having a specification determined in accordance with the computer service or services requested by said customer and being configurable by said customer, said at least one virtual machine having an operating system running thereon.

55. (Original) A method according to claim 54, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer.

56. (New) Apparatus according to claim 1, wherein at least one of said virtual machines provides at least a virtual central processor unit.

57. (New) Apparatus according to claim 1, wherein at least one of said virtual machines is created using a virtual machine abstraction program.

58. (New) Apparatus according to claim 1, wherein at least one of said virtual machines is created using machine simulation/emulation software.

59. (New) A method according to claim 20, wherein at least one of said virtual machines provides at least a virtual central processor unit.

60. (New) A method according to claim 20, wherein at least one of said virtual machines is created using a virtual machine abstraction program.



App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

61. (New) A method according to claim 20, wherein at least one of said virtual machines is created using machine simulation/emulation software.
62. (New) A method according to claim 37, wherein at least one of said virtual machines provides at least a virtual central processor unit.
63. (New) A method according to claim 37, wherein at least one of said virtual machines is created using a virtual machine abstraction program.
64. (New) A method according to claim 37, wherein at least one of said virtual machines is created using machine simulation/emulation software.

App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

### REMARKS/ARGUMENTS

Applicant acknowledges receipt of the Office Action dated December 9, 2004, in which the Examiner objected to claim 53, rejected claims 1-3, 10-11, 13, 18-22, 28-29, 31, 36-39, 45-46, 48 and 53-55 as obvious over Bugnion (US 6075938) in view of Derks (US 6810033 B2); and rejected claims 4-9, 12, 14-17, 23-27, 30, 32-35, 40-44, 47 and 49-52 as obvious over Bugnion (US 6075938) in view of Derks (US 6810033 B2) in combination with Bowman-Amuah (US 6697824).

Applicant thanks the Examiner for her thoroughness in preparing the Office Action. At the same time, Applicant respectfully submits that the rejections of the present claims must fail for the reasons set out below.

#### Status of the Claims

Independent claims 1, 20, 37, and 54 have been amended. Of the original dependent claims, only claim 53 has been amended. New claims 56-64 are added. Claims 1-64 are pending.

#### Rejections under 35 U.S.C. § 103(a)

In support of her rejection of claims 1-3, 10-11, 13, 18-22, 28-29, 31, 36-39, 45-46, 48 and 53-55 as obvious over Bugnion in view of Derks, the Examiner asserts that Bugnion teaches "providing one or more computer services for a plurality of customers, the apparatus comprising a real computer on which is set up of each of said customers [sic] at least one virtual machine for each of said customers." Applicant respectfully submits that this rejection is based on a fundamental misunderstanding on the part of the examiner as to what is claimed in the present application and what is disclosed in the cited art.

First, each independent claim in the present application requires a "virtual machine." In the context of the present invention, the term "virtual machine" is used to refer generally to the technology by which software is written and executed on a real computer in order to create a virtual computer on which an operating system runs. This is described in a number of places throughout the present specification and the examiner is referred particularly to the passage at page 17, line 25 to page 18, line 27 of the present description. Thus, in the sense used in the present specification, a virtual machine is a practically self-contained operating environment that behaves as if it is a separate computer, separately of the real or physical computer on which the software that generates the virtual machine is run.

App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

In the context of the present invention, Bugnion discloses no more than an efficient piece of software for creating virtual machines. With respect to the present invention, Bugnion has no more relevance than any other software or other technology for creating virtual machines. The examiner will certainly know, and indeed the present specification states, that virtual machine technology per se is not new. Correspondingly, virtual machine monitors themselves are not new. As mentioned on for example page 17 of the present application and at column 2, lines 36 onwards of Bugnion, IBM developed virtual machine technology in the late 1960s and early 1970s. Bugnion was cited in the present application as filed and Applicant is confident that there is no disclosure nor suggestion of the present invention in Bugnion.

Specifically, Bugnion does not disclose providing one or more computer services for a plurality of customers, or setting up at the request of each of said customers at least one virtual machine for each of said customers, the at least one virtual machine for each of said customers having a specification specified by the respective customer (emphasis added). Nowhere does Bugnion disclose or suggest the concept of creating plural virtual machines on a real computer in which at least one virtual machine is set up for each of the customers, each of those virtual machines having a specification that is specified by the respective customer.

It appears that the examiner is equating the term "customer" in the claims of the present application with "applications" in the sense of "software applications" in Bugnion. Applicant respectfully submits that there is no basis for this comparison. In no sense can a "customer" be equated with or be considered to be analogous to a "software application." Contrary to the examiner's assertion, this is not a mere implementation detail, but rather goes to the heart of the present invention.

The principal problem that is addressed by the present invention is how to host or provide computer services (such as applications hosting services, web hosting services, etc., as detailed in the present application) for plural customers in a secure way while minimizing the real physical resources which are required. This is a significant and very real and current technical problem. At present, those who are providing such hosting services for third parties typically have very many real computers, with a respective real computer being dedicated to each customer. This has significant cost and maintenance implications for the provider, which inevitably results in relatively high costs being passed onto the customers. The present invention solves this technical

App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

problem with a technical solution, namely the creation and use of plural virtual machines for the respective customers.

Bugnion does not disclose nor suggest using virtual machines in this manner. The examiner may know that, historically, virtual machines were used almost exclusively by computer scientists, especially when developing new software. The computer scientists would typically create a virtual machine on a real machine and use the virtual machine to develop and test new software (such as operating systems and software applications). Plural virtual machines might be set up, with each running different versions of the software. The main advantage of using the virtual machine rather than the real computer was that if the software being developed caused problems to the operating system running on the virtual machine or to the virtual machine itself, then only the virtual machine would "crash", and the underlying real computer would not be affected at all. Thus, computer scientists could safely develop new software without concern as to whether the new software might cause problems for the real computer. The examiner will immediately appreciate the inconvenience of a real computer crashing, owing to the delay in restarting the computer and the like and because of the possibility of serious and irrecoverable damage being caused to the real computer. In short, virtual machine technology was developed by and for computer scientists, were of very little interest to those working outside the field of computer science, and were principally of interest only to a few software developers and academics.

Thus, while the present invention makes use of technology that per se is old (i.e. virtual machine technology), the present invention uses that technology in a new and non-obvious way to enable persons to provide or host computer services for plural customers, thus providing a technical solution to this technical problem.

The virtual machines of the present invention can be isolated from each other so as to operate in a secure manner, so that for example one customer does not have any access to the applications or services being hosted for other customers even if they are running on the same physical computer. The use of plural virtual machines also provides for enormous efficiency in use of physical resources, such as real memory, real storage (such as hard disks or tape or the like), real CPUs, etc., because the physical resources can effectively be spread over plural customers. Moreover, if a customer's requirements change so that more storage, more memory, higher processing speed, etc., are required, this is easily accommodated by modifying the set-up of the

App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

virtual machine and does not (normally) require that new physical apparatus be purchased by the operator of the real computer. This allows customers to have effective access to the latest processors, data storage devices, memory devices, etc. at relatively low cost as the cost of the real resources can effectively be spread across plural customers. Such advantages are amply described in the present application and the examiner is referred for example to the section from page 29, line 4 to page 31, line 19 of the present application.

The other main document cited by the examiner, Derks, does not even refer to virtual machines. This patent relates to what is referred to in the patent as "Private Virtual Networking", which is more commonly known as "virtual private networking" or "VPN", which relates solely making a secure transmission channel over an insecure network. This has nothing whatsoever to do with virtual machine technology. Even at the passages cited by the Examiner, Derks makes no teaching or disclosure of a virtual machine for each customer or of the virtual machine having a specification specified by the customer. Hence, the combination of Derks with Bugnion simply *does not support* the present obviousness rejection.

In order to clarify the aforementioned distinctions, each pending independent claim has been amended to require that the at least one virtual machine for each of the customers have a specification specified by and configurable by the respective customer. Support for this amendment can be found in several places in the specification, including for example page 16, lines 24 to 26 and page 26, lines 11 to 15 of the present application. The independent claims have also been amended to recite virtual machine(s) "having an operating system running thereon." This amendment is intended to clarify that the claims relate to virtual machine technology proper, as discussed above. Support for this amendment can be found at *inter alia* page 17, line 26 onwards.

For all of the foregoing reasons, it is respectfully submitted that the invention of each independent claim is patentable. Because the rejection of the independent claims must fail, the rejection of claims 4-9, 12, 14-17, 23-27, 30, 32-35, 40-44, 47 and 49-52 as obvious over Bugnion in view of Derks in combination with Bowman-Amuah must also fail.

#### New Claims

New dependent claims 56 to 64 have been added to specify further preferred details of virtual machine technology in the context of the present invention.

App. No.: 09/898,286  
Reply to Office Action of December 9, 2004

Claims 56, 59 and 62 refer to a virtual machine providing a virtual central processor unit, support for this amendment being found at *inter alia* page 18, lines 12 and 13 and page 29, lines 11 to 14.

Claims 57, 60 and 63 refer to a virtual machine being created using a virtual machine abstraction program, support for this amendment being found at *inter alia* page 16, line 21.

Claims 58, 61 and 64 refer to a virtual machine being created using machine simulation/emulation software, support for this amendment being found at *inter alia* page 23, line 18 to page 24, line 11.

Because they depend from allowable base claims, and because they set out further limitations that distinguish them over the art, new claims 56-64 are also allowable.

#### Conclusion

Applicant respectfully submits that the claims are in condition for allowance. If the Examiner has any questions or comments, or otherwise feels it would be advantageous, he is encouraged to telephone the undersigned at (713) 238-8043.

Respectfully submitted,



Marcella D. Watkins

Reg. No. 36,962

Conley, Rose P.C.

P. O. Box 3267

Houston, Texas 77253-3267

(713) 238-8000

ATTORNEY/AGENT FOR APPLICANT

# EXHIBIT B

FROM : LAW OFFICE SHERMAN L PERNIA

FAX NO. : 281-333-9144

Apr. 17 2005 09:27AM P5

claim under consideration." It is not enough, however, that the prior art reference disclose all the claimed elements in isolation. Rather, as stated by the Federal Circuit, "[a]nticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, *arranged as in the claim*." Further, under 35 USC §102, anticipation requires that "... the prior art reference must be enabling, thus placing the allegedly disclosed matter in the possession of the public." The Federal Circuit has added that: "There must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention." *Scripps Clinic & Research Found. v. Genentech Inc.*, 18 USPQ 2d 1001, 1010 (Fed. Cir. 1991).

The Office holds independent claim 1 as being anticipated by the '962 patent contending that Touboul discloses all of the elements of instant claim 1.

However, Applicants assert that the Touboul '962 patent: (1) does not disclose all of the elements (or their equivalents) of instant claim 1 functioning in the same way as the claimed invention; (2) does not disclose each and every element of the claimed invention *arranged as in the instant claim*. Additionally, Applicants assert that there are difference between the claimed invention and the '962 patent disclosure, as viewed by one of ordinary skill in the art at the time of the invention by Applicants. Applicants submit Tables I & II and the following remarks showing the failure of the cited reference to satisfy the requirement of "strict identity" for a §102 reference.

Table I shows the cited reference's requirement for a "communications channel" element, whereas the invention of instant claim 1 has no such requirement, and its protection features are enabled and function without a server and/or a communications channel, because the present invention does not depend on the hostile download coming via a communications channel in order to provide protection from hostile downloads. Omission of an element with retention of the element's function is indicia of unobviousness. *In re Edge*, 359 F.2d 896, 149 USPQ 556 (CCPA 1966).

Docket #: EXOB-216R-1

-3-

PAGE 5/11 \* RCVD AT 4/17/2005 10:18:48 PM [Eastern Daylight Time] \* SVR:USPTO-EFAXP-1/0 \* DNIS:8720300 \* CSID:281 333 9144 \* DURATION (mm-ss):08-04

PAGE 34/39 \* RCVD AT 12/28/2005 10:22:52 PM [Eastern Standard Time] \* SVR:USPTO-EFAXP-6/24 \* DNIS:2738300 \* CSID:7132288778 \* DURATION (mm-ss):08-54



FROM : LAW OFFICE SHERMAN LERNIA

FAX NO. : 281-333-9144

Apr. 17 2005 09:28PM PG

TABLE IA Identity Comparison of Required Elements			
Instant claim 1:	The Touboul System (100), see Fig. 1:	Is the Language:	
		Identical?	Equivalent?
Omitted	a server (110) and a communications channel (120)	NO	NO
an intrusion secure computer system	a client (130) with a security system (135)	NO	MAYBE

As disclosed in the '962 patent (at col. 2, line 61 to col. 3, line 8 and in Fig.1), the Touboul system requires that the "hostile" downloadable (140) from which the client (130) is protected come via a network communications connection (120). In contrast, the present invention of instant claim 1 does not require a server nor a communications connection to be able to protect a client from a hostile downloadable. This is an elemental difference between the present invention and the Touboul system. The present invention of instant claim 1 will protect the client from hostile downloadables on a floppy disk inserted into a client's floppy drive. The Touboul '962 patent does not teach or suggest this, nor can it be adapted to accomplish this because of the fundamental differences between the structure and function of the present invention and the Touboul system. Likewise, the present invention protects the client from hostile downloadables from optical disks and other external data storage media. The Touboul system cannot do this. Some of the reasons for this are set forth below.

Because the present invention of instant claim 1 does not require a communications connection nor a server, as does the disclosed Touboul system, there is not strict identity between the Touboul disclosure and the instant claims, and therefore, the present invention is not *prima facie* anticipated by the '962 patent reference.

Docket #: EXOB-216R-1

-4-

PAGE 35/39 \* RCVD AT 4/17/2005 10:18:48 PM [Eastern Daylight Time] \* SVR:USPTO-EFXXRF-1/0 \* DNIS:8726308 \* CSID:281 333 9144 \* DURATION (mm-ss):08-04

PAGE 35/39 \* RCVD AT 12/28/2005 10:22:52 PM [Eastern Standard Time] \* SVR:USPTO-EFXXRF-6/24 \* DNIS:2738300 \* CSID:7132288778 \* DURATION (mm-ss):08-54